AUTOSAR at the cutting edge of automotive technology

01 December 2011
The 32nd IEEE Real-Time Systems Symposium (RTSS)

Dr. Bert Bögdeker – DENSO AUTOMOTIVE Deutschland GmbH
Dr. Rafael Zalman - Infineon Technologies AG, Automotive Electronics
- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words
Automotive Context

AUTOSAR Introduction

Automotive Challenges
- Cost
- Functional Safety
- Energy Efficiency
- Multi-Core

Research Example: parMERASA

Research Landscape

Closing Words
Automotive Numbers

- Total estimated number of cars on the street worldwide ≈ 600 millions
- G7 countries have 749 vehicles / 1000 people
- Around 87% of total motor vehicles are passenger cars

**Car production worldwide:**

<table>
<thead>
<tr>
<th>Year</th>
<th>Annual Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>1997</td>
<td>40,000,000</td>
</tr>
<tr>
<td>1998</td>
<td>50,000,000</td>
</tr>
<tr>
<td>1999</td>
<td>60,000,000</td>
</tr>
<tr>
<td>2000</td>
<td>70,000,000</td>
</tr>
<tr>
<td>2001</td>
<td>80,000,000</td>
</tr>
<tr>
<td>2002</td>
<td>77,857,705</td>
</tr>
</tbody>
</table>

Source: OICA
Estimated ECU Volume 2009 (K)

<table>
<thead>
<tr>
<th>Country</th>
<th>Volume (K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turkey</td>
<td>2,608</td>
</tr>
<tr>
<td>Thailand</td>
<td>2,904</td>
</tr>
<tr>
<td>Russia</td>
<td>3,612</td>
</tr>
<tr>
<td>Iran</td>
<td>4,186</td>
</tr>
<tr>
<td>Poland</td>
<td>4,395</td>
</tr>
<tr>
<td>Belgium</td>
<td>5,228</td>
</tr>
<tr>
<td>Mexico</td>
<td>7,786</td>
</tr>
<tr>
<td>Italy</td>
<td>8,432</td>
</tr>
<tr>
<td>Czech Rep.</td>
<td>9,745</td>
</tr>
<tr>
<td>India</td>
<td>10,530</td>
</tr>
<tr>
<td>UK</td>
<td>10,901</td>
</tr>
<tr>
<td>Brazil</td>
<td>12,730</td>
</tr>
<tr>
<td>Canada</td>
<td>14,896</td>
</tr>
<tr>
<td>South Korea</td>
<td>17,564</td>
</tr>
<tr>
<td>France</td>
<td>20,497</td>
</tr>
<tr>
<td>Spain</td>
<td>21,700</td>
</tr>
<tr>
<td>China</td>
<td>27,581</td>
</tr>
<tr>
<td>Japan</td>
<td>79,345</td>
</tr>
<tr>
<td>United States</td>
<td>85,677</td>
</tr>
<tr>
<td>Germany</td>
<td>104,197</td>
</tr>
</tbody>
</table>

$\sum \approx 450$ million electronic control units/ year
- Vehicles have a long life cycle – state of the art = 25 years
- Electronic components have a dramatically shorter life cycle
- Impact on the SW architectures!
  - Standardization of SW architectures
  - HW independent specification of SW functions
  - Updates = SW life cycle is shorter than ECU life cycle
  - Robustness instead of fast innovation

Vehicle life cycle typical values:
- DEVELOPMENT: 3 years
- PRODUCTION: 7 years
- OPERATION & SERVICE: 10 - 15 years

Just orientation values – may differ for concrete examples
Automotive Context

- AUTOSAR Introduction

Automotive Challenges

- Cost
- Functional Safety
- Energy Efficiency
- Multi-Core

Research Example: parMERASA

Research Landscape

Closing Words
AUTOSAR Introduction

Core Members

- Bayerische Motoren Werke AG
- Robert Bosch GmbH
- Continental AG
- Daimler AG
- Ford Motor Company
- General Motors Holding LLC
- Peugeot Citroën Automobiles S.A.
- Toyota Motor Corporation
- Volkswagen AG

Premium Members

- ALTRAN Group
- Autoliv
- B2i
- CEA List
- Dassault Systèmes
- Delphi Corporation
- Denso Corporation
- dSpace GmbH
- Elektrobit Group Plc
- ETAS Entwicklungs- und Applikationswerkzeuge für elektronische Systeme GmbH
- Electronics and Telecommunication Research Institute(ETRI)
- Fiat Auto S.p.A.
- Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
- Freescale Semiconductors
- Hella KGaA Hueck & Co.
- Honda Motor Co., Ltd. & Honda R&D Co., Ltd.
- Hyundai Motor Company
- IAV
- IBM Corporation
- INCHRON GmbH
- Infineon Technologies AG
- Intecs- Informatica e Tecnologia del Software SpA
- Johnson Controls GmbH
- JTEKT CORPORATION
- KPIT Cummins Infosystems Limited
- M/S Larson & Toubro Limited
- Lear Corporation
- Magna International Inc.
- Magneti Marelli Holding S.p.A
- Mazda Motor Corporation
- MB-Technology GmbH
- Mentor Graphics Corporation
- NXP B.V.
AUTOSAR Standardization areas

Software & Architecture
- Automotive Basic Software
- Run Time Environment (RTE)

Methodology
- Virtual Function Bus (VFB)
- Configuration Language

Application interfaces
- all application domains
Automotive Context

AUTOSAR Introduction

Automotive Challenges
- Cost
- Functional Safety
- Energy Efficiency
- Multi-Core

Research Example: parMERASA

Research Landscape

Closing Words
Vast majority of software development effort is spent on adaptation of existing solutions.
Reusability of software

Integration by configuration

Built in variant handling
→ Software product lines

Components with standard format
→ Reuse for different suppliers
→ Reuse for different car lines

Layered architecture
→ Reuse for different HW

Standard interfaces & behavior
→ Mature implementations
→ Implementations shared by many OEMs

Application Layer

Runtime Environment

Basic Software
Reusability of software still required:

- Components with standard format → Reuse for different suppliers
  → Reuse for different car lines
- Assume guarantee pattern (→FAT AK31)
  → Reusable certification
  → Easy integration
- Application interfaces (Semantic)
  → Reuse for different OEMs
- Layered architecture
  → Reuse for different HW
- Standard interfaces & behavior
  → Mature implementations
  → Implementations shared by many OEMs

Integration by configuration
- Built in variant handling
  → Software product lines

Whole PLM approach (→AMALTHEA)

Application interfaces (Semantic) → Reuse for different suppliers
- Reuse for different car lines

Background

AUTOSAR Standard

Research

Basic Software

Runtime Environment

Application Layer
- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words
Functional Safety

Background

Safety is absence of unreasonable risk

- Society judges the level of acceptable risk

Functional Safety is the absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems*

- Avoid malfunctions of E/E systems
- Applicable to all E/E systems with intrinsic risks

*) ISO 26262-1
Scope of ISO26262

**Target**
- Passenger cars < 3.5t
- OUT: Trucks, Motorbikes, Tractors,…

**Object under consideration**
- E/E System device, semiconductor, hardware design, software
- OUT: mechanic structure, material

**Hazards under consideration**
- Human damage
- OUT: material damage

**Faults under consideration**
- Systematic design faults, random hardware faults, etc.
- OUT: abnormality due to high voltage, ageing, fire hazard, heat, corrosion, performance
Background

Standard: ISO 26262
Road vehicles — Functional safety
Parts:

1. Vocabulary

2. Management

3. Concept phase

4. Product development at the system level

5. Product development at the hardware level

6. Product development at the software level

7. Production and operation

8. Supporting processes

9. ASIL-oriented and safety-oriented analysis

10. Guideline on ISO-26262
Purpose of ISO 26262

What it is **not**:
- Certification requirement

What it is **partially**:
- Legal requirement
  - only through product liability requirement for ‘state of the art’

What it **is**:
- Guidance to find right level of functional safety effort to spend.
  - Reduce number of **callbacks** for safety reasons.
- Defense against liability claims.
Disclaimer

AUTOSAR (AR) does NOT guarantee any Functional Safety (FS) properties of the final system

- AR provides mechanisms to support FS (SW level)
- Helps during the design phase for SW level
- Each system has its own context of use, functionality and implementation

The full responsibility for selecting and implementing appropriate safety mechanisms as described inside the AUTOSAR framework fully resides on the implementer.
Partitioning
- Memory protection
- Timing protection (time budgets)
- Selective stop of partitions for increased critical function availability

Permits separation
- Mixed safety integrity levels
- Responsibility sharing across SW vendors

AUTOSAR Standard

Functional Safety
End to End Communication Protection

- Provides
  - Data integrity,
  - Authentication,
  - Sequence check

- Implemented by
  - Static end to end protection library
  - Wrapper code for handling protection context for communication
Program flow

Watchdog manager
- Check alive
- Check correct sequence
- Check transition deadline

E.G., reset ECU using watchdog driver
A problem has been detected and Windows has been shut down to prevent damage to your computer.

If you see this stop error screen,

1. Restart your computer.
2. If this screen appears again, follow these steps:

   a. Check to make sure any new hardware or software is properly installed.
   b. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.
   c. If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing.
   d. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x00000000, 0x0000002, 0x00000000, 0xF86B5A89)

*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.
Availability / fault operational concepts

- Safety related extensions for methodology
  (SAFE, AR internal)

- Use of multi core for hardware partitioning

- Runtime HW tests integration

- Convergence of safety & security
  (SESAMO proposal)

Safe and reliable integration of components
(TIMMO-2-USE, recomp).

- Safe and robust software execution (AR internal)
Scheduling effects are already complex in small systems
- More complex in multi cores

Fulfillment of timing constraints must be checked
- Already in single cores and even more in multi cores
- Scheduling Analysis is one way
- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words
# Energy Efficiency

**Background**

*EC CO₂ Emissions Regulation 443/2009*

<table>
<thead>
<tr>
<th>100 W electrical</th>
<th>0.1 l/100km</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 kg</td>
<td>0.1 l/100km</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1 l/100km Fuel</th>
<th>23.6 g CO₂/km</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 l/100km Diesel</td>
<td>26.5 g CO₂/km</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1 g CO₂/km</th>
<th>40 W electric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 g CO₂/km</td>
<td>20 kg</td>
</tr>
</tbody>
</table>

| 1 g CO₂/km       | 95 €*         |

- Similar battery cost results for electric cars

- Current consumption per ECU ~200 mA

- 40 W or 20 kg

- 1 g CO₂/km

- 95 € fine

Copyright © DENSO CORPORATION and Infineon Technologies 2011. All rights reserved.
Partial Networking

Many Functions are only sporadically required:
- Seat heating
- Trailer connector
- Window lifter
- In total: ~10 ECUs

Idea:
- Turn off all nodes that do not contribute to any active function
Partial Networking

Challenges:

- Methodology to map functions to software component and communication resources
- Bookkeeping of active functions / partial network clusters
- Coordinate partial communication
- Coordinate sleep and selective wakeup of some nodes
ECU local measures (to be published in rev. 4.04)
vehicle mode architecture:
How to consistently control vehicle resources and vehicle functions with contradicting optimization criteria like energy consumption, comfort, safety, …
Automotive Context

AUTOSAR Introduction

Automotive Challenges

- Cost
- Functional Safety
- Energy Efficiency
- Multi-Core

Research Example: parMERASA

Research Landscape

Closing Words

Technology

- Multi-core
- ...

Content

RTSS 2011
Background

Multi Core Benefits

Image removed
Multi Core – Energy efficiency & performance

- Dual (multi) core is the solution to the Moore law & power dissipation problem.

\[ P_{d} \sim C \cdot U^2 \cdot f \]
Background

Example Concept for Hybrid Architecture

- Safe Processing Concept (Aurix, Infineon)
- Lockstep application processor
- Lockstep peripheral control processor
- able to run diversity mode
- memory management for Cores and DMA have,
- ECC protection for memory and busses
- scalable and composable in performance and memory size
Multi Core Support

- Single image OS
- Tasks and software components bound to cores
- Shared memory assumption (not exploited)
- Generic module for inter core communication (IOC)
- Spin-locks for explicit synchronization
Automotive related multi-core research

- How to scale with large number of cores (TERAFLUX)
- Load balancing
- (Semi-) Automatic parallelization
- Better scheduling mechanisms than local PCP and spin locks.
  - Predictable multi core scheduling (parMERASA)
Content

- Automotive Context
- AUTOSAR Introduction
- Automotive Challenges
  - Cost
  - Functional Safety
  - Energy Efficiency
  - Multi-Core
- Research Example: parMERASA
- Research Landscape
- Closing Words
Multi-Core Execution of *parallelised* Hard Real-Time Applications Supporting Analysability

EC FP-7 project 2011-2014
start: Oct. 1, 2011
3.3 Mio EC contribution

Project webpage: [http://www.parmerasa.eu](http://www.parmerasa.eu)
Background

AUTOSAR Standard

Research

Project partners

- University of Augsburg (Project Coordinator)
- Barcelona Supercomputing Center
- Université Paul Sabatier
- Technical University of Dortmund
- Rapita Systems Ltd.
- Honeywell international s.r.o.
- BAUER Maschinen GmbH
- DENSO AUTOMOTIVE Deutschland GmbH
parMERASA Industry Advisory Board

- Benoit Triquet, Airbus,
- Philippe Chevalley, European Space Agency ESA,
- Glenn Farrall, Infineon Technologies UK Ltd,
- Rafael Zalman, Infineon Technologies AG,
- Andre Lajtkep, BMW Group,
- Hakan Sivencrona, MECEL AB,
- Claus Stellwag, Elektrobit Automotive GmbH,
parMERASA relevance for automotive

- How to parallelize automotive applications while preserving the real time properties?
- Safe scheduling (not only in multi core ECUs)
- Where are the limits for parallelization of automotive applications?

Use cases
- Fuel efficient engine control
- Vehicle internal router
- High integration - compound ECU
Automotive Context

AUTOSAR Introduction

Automotive Challenges
- Cost
- Functional Safety
- Energy Efficiency
- Multi-Core

Research Example: parMERASA

Research Landscape

Closing Words
Incomplete list of automotive related research projects

- Cost
  - Reusability
  - Efficiency

- CESAR
- AMALTHEA
- RECOMP
- TIMMO2USE
- SAFE
- SAFE -E
- parMERASA
- Performance
- TERAFLUX
Automotive Context

AUTOSAR Introduction

Automotive Challenges
- Cost
- Functional Safety
- Energy Efficiency
- Multi-Core

Research Example: parMERASA

Research Landscape

Closing Words
The automotive industry has found in AUTOSAR a standardization body for standardization of their system and software architecture framework.

Innovations are brought in from public research projects

Future concerns of AUTOSAR:

- **Fragmentation**: How to master different releases, how to prevent cherry picking and simplified subsets in BRICS?
- **Ageing**: Easy to integrate innovations, difficult to clean up